Evaluating Damages Caused by Information Systems Security Incidents

Fariborz Farahmand[1], Shamkant B. Navathe[2], Gunter P. Sharp[3], Philip H. Enslow[4]

Georgia Institute of Technology, Atlanta, GA

Abstract

As organizations adopt increasingly sophisticated information systems, the challenge of protecting those systems becomes enormous. Accordingly, the single critical decision security managers have to make is the amount an organization is willing to spend on security measures to protect assets of the organization. To arrive at this decision, security mangers need to know explicitly about the assets of their organizations, the vulnerability of their information systems to different threats, and their potential damages.

Each threat and vulnerability must be related to one or more of the assets requiring protection. This means that prior to assessing damages we need to identify assets. Logical and physical assets can be grouped into five categories: 1) Information- Documented (paper or electronic) data or intellectual property used to meet the mission of an organization, 2) Software- Software applications and services that process, store, or transmit information, 3) Hardware- Information technology physical devices considering their replacement costs, 4) People- The people in an organization who posses skills, knowledge, and experience that are difficult to replace and, 5) Systems- Information systems that process and store information (systems being a combination of information, software, and hardware assets and any host, client, or server being considered a system).

Various units of value or metrics for valuation of assets may be used. The common metric is monetary, which is generally used for data that represent money where the threat is direct financial theft or fraud. Some assets are difficult to measure in absolute terms but can be measured in relative ways, for example information. The value of information can be measured as a fraction or percentage of total budget, assets, or worth of a business in relative fashion. Assets may also be ranked by sensitivity or

1- Ph. D. Student, ff@cc.gatech.edu
2- Professor, sham@cc.gatech.edu
3- Associate Professor, gsharp@isye.gatech.edu
4- Professor Emeritus, enslow@cc.gatech.edu

importance to an organization in relative ways. The authors believe that 1) Destruction of information and/or other resources, 2) Corruption or modification of information, 3) Theft, removal or loss of information and/or other resources, 4) Disclosure of information; and 5) Interruption of services; are major categories of threats to the information systems.

The impact of information security incidents may well be financial, in forms of immediate costs and losses of assets. For example, the cost of downtime per hour caused by a denial of service attack can be computed by measuring the loss of:

Productivity: (Number of employees impacted) × (hours out)
× (burdened hourly rate)

Revenue: Direct loss, lost future revenues

Financial Performance: Credit rating, stock price

Other Expenses: Equipment rental, overtime costs, extra shipping costs,
travel expenses, etc.

But, much more serious are the hidden costs. Consider the example of denial of service attack, where the damaged reputation of the company can have negative impact on the relationship of the company with its customers, suppliers, financial markets, banks, and business partners. These hidden costs are extremely difficult to quantify and to measure. Others suggest qualitative or quantitative approaches for these kinds of evaluations. However, qualitative or quantitative risk analysis in information security has its pros and cons.

We overview the existing classifications of the threats to the information systems and some of their shortcomings. We also present a more comprehensive classification of the threats and some security measures to confront them. In this classification, threats are considered from two points of view: 1- Threat agent, and 2- Threat technique. Threat agent could be environmental factors, authorized users, unauthorized users and threat (penetration) technique could be personnel, physical, hardware, software, or procedural.

We believe that the cost of an information system security incident on a company has to be measured in terms of the impact on its business; hence identical incidents in two different companies could have different costs. To evaluate these costs and measure the impact of a security incident on a company, we need a systematic approach and a comprehensive risk management system. Such a comprehensive security risk evaluation system is currently under development at the College of Computing, Georgia Institute of Technology. This system with five stages is aimed at helping managers to identify the vulnerabilities of their companies and to select the countermeasures and it includes: 1- Resource and application value analysis, 2- Vulnerability and risk analysis, 3- Computation of losses due to threats and benefits of countermeasures, 4- Selection of countermeasures and 5- Evaluation of implementation alternatives

In previous papers the authors have presented a subjective analysis and probability assessment approach as a possible solution for vulnerability assessment and damage evaluation of information security incidents. We provide a model of classification of security threats and develop a three-axis view of the threat space and a scheme for probabilistic evaluation of impact of the security threats. We present an analysis of five incidents. The agents and threats are classified and related to the damages within each organization.